Energy Provider Community of Interest September 2015

Securing Networked Infrastructure for the Energy Sector

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Monthly Call Agenda

- Identity and Access Management (IdAM) project update
- Situation Awareness (SA) project update

Contact us at energy_nccoe@nist.gov

OVERVIEW: ENERGY SECTOR USE CASES

Identity and Access Management (IdAM)

- Authenticate individuals and systems
- Enforce authorization control policies
- Unify IdAM services
- Protect generation, transmission and distribution

Situational Awareness

- Improve OT availability
- Unify visibility across silos
- Detect anomalous conditions and remediate them
- Investigate events leading to anomalies and share findings

PROJECT MILESTONES

Identity and Access Management

- Draft Practice Guide released: 08/25/2015
- Comment Period: 60 days
- Build Demonstration: October 2015
- Final Guide Release: December 2015

Situational Awareness

- Finalize List of Collaborators: September 2015
- Situational Awareness Architecture: October 2015
- Draft Practice Guide: March 2016

Identity and Access Management (IdAM) Draft Practice Guide Update

- Draft practice guide released August 25!
- Find the draft guide online at https://nccoe.nist.gov/projects/use_cases/idam
- Please submit comments (deadline October 23):
  - Do you believe NCCoE has properly identified a serious security concern within the energy industry?
  - Does the practice guide effectively address a serious security concern *within your organization*?
  - What would be the biggest obstacle to adoption of this solution, as a whole or in part?
  - If the NCCoE were to consider subsequent iterations of this practice guide, what would you suggest as the core focus?

Practice Guide Campaign Statistics

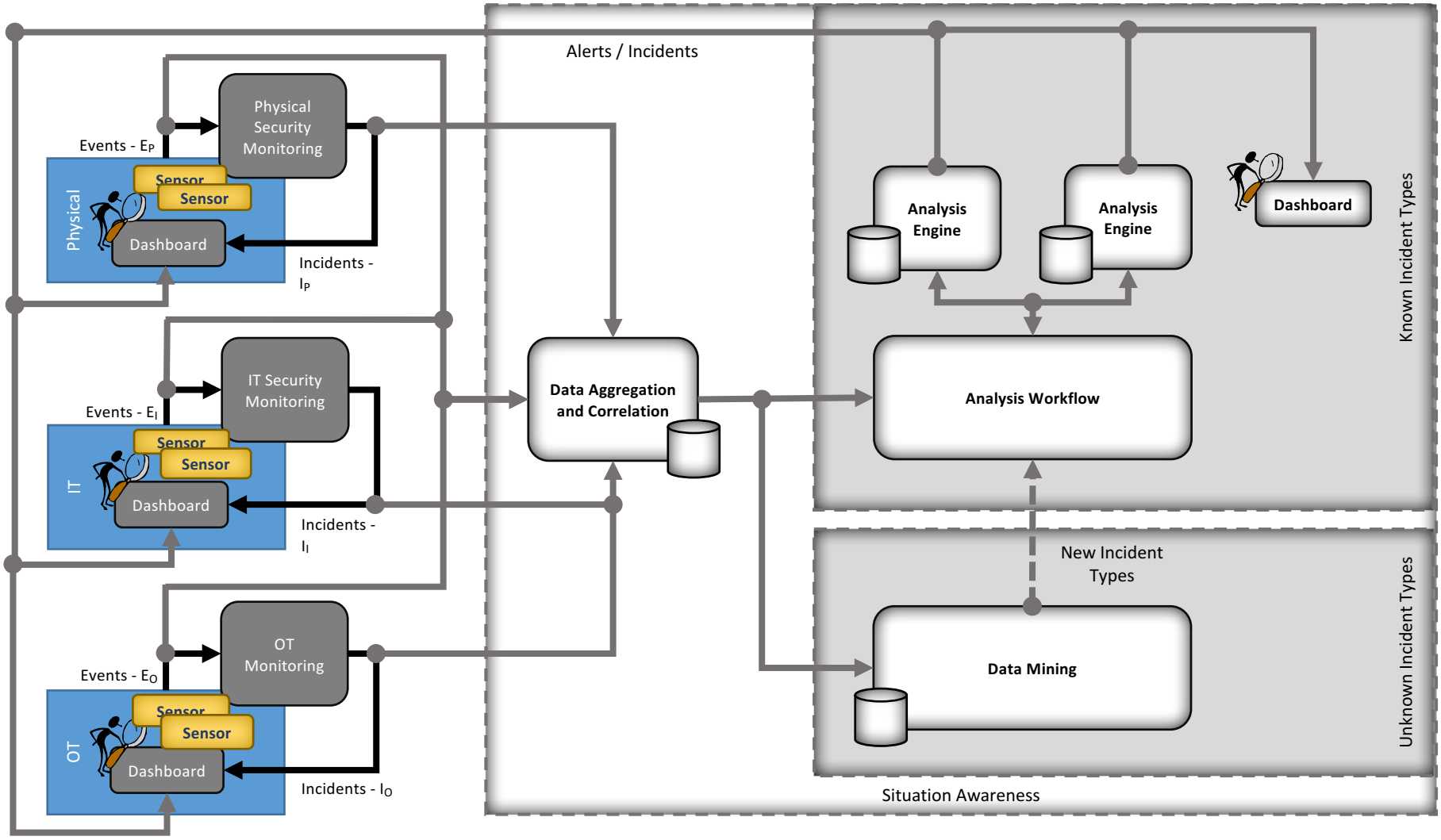
- ES IdAM Project Web page stats:
  - **3,124 visits to project page**
- IdAM Guide Downloads
  - 1800-2a Executive Summary: 182
  - 1800-2b Approach: 185
  - 1800-2c How-To Guide: 167
  - ES IDAM Use Case (zip file): 176
  - **Total downloads since release: 2190**
- News Articles:
  - Computer World: http://www.computerworld.com/article/2975934/security/us-agency-warns-electric-utilities-to-bolster-authentication.html
  - NextGov: http://www.nextgov.com/cybersecurity/2015/08/feds-urge-energy-companies-ramp-cyber-protections/119594/?oref=ng-channelriver
  - DailyDot: http://www.dailydot.com/politics/cybersecurity-nist-energy-security-proposal/
  - Environment & Energy News: http://www.eenews.net/stories/1060023939
  - SANS News Bites: https://www.sans.org/newsletters/newsbites/xvii/67#306

What's Next?

- Demonstration of solution for your organization
- Customized review of practice guide with your organization
- Are we doing good work? Help us get the word out!
  - Email copy available for you to send to your colleagues
  - Social media posts available for you to use

Contact us at energy_nccoe@nist.gov

Notional Build – Centralized Management



What's Next?

- Collaborate with Project Team on build planning
- Receive and consider input to use case from Energy Provider Community of Interest
- Finalize project build architecture

CLOSING


240-314-6800
http://nccoe.nist.gov/forums/energy
Thank You
energy_nccoe@nist.gov
9600 Gudelsky Drive
Rockville, MD 20850

ABOUT THE NCCOE

National Institute of Standards and Technology
U.S. Department of Commerce

Information Technology Laboratory

MARYLAND OF OPPORTUNITY.®
Department of Business & Economic Development

MONTGOMERY COUNTY
17 76
GARDEZ BIEN
MARYLAND

WHO WE ARE AND WHAT WE DO

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on a combination of multiple commercially available technologies

Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)

TENETS

Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards

Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

PROJECT LIFECYCLE